[Detailed Description of the Invention]

[0001]

[Field of the Invention]

The present invention relates to the information processor managing file security.

[0002]

[Prior Art]

In the clients (information processor) without security device of the conventional technology, a pass word is written in every file recoded in the disk device, FD (Floppy Disk Media), and MO (Magneto Optical Disk). When the clients receive a request of the file access, the pass word is entered by the user, and if the pass word conforms, the permission is given to the user for the file access. Thus the files ensured security.

[0003]

[Problems to be Solved by the Invention]

In the above described clients without security device where the pass word is written in the respective files, and when the clients receive a request of the file access the pass word is entered by the user, and if the pass word conforms, the permission of the file access is given to the user. Thus, it is a big burden on users to set the pass word, to confirm the pass word, and to change the pass word. Moreover, the pass word is written in each of the files, thus the security management is restricted to a personal file, therefore, it is difficult to manage the security of the files by unit of the department or by unit of the division in the company organization.

[0004]

The object of the present invention is, in order to eliminate the above problems, managing the security of the information processor without security device where a domain name and security information on the owner ID, group name, and whether the group has the access right are written in the respective files, and thus the security is managed based on them.

[0005]

[Means to Solve the Problems]

A description will be given of the means to solve the problems with reference to Fig.1. The registering means 12 shown in Fig.1 is where the data, domain name, and security information are registered in a file, and a predetermined domain name is registered in the apparatus.

[0006]

The access right confirming means 13 is where the access right is confirmed according to the domain name and security information stored in the file. Next, the operation will be described.

[0007]

When a request for access is made, the access right confirming means 13 reads the security information from the requested file, and then collates the input information and the security information which is read from the file, and

if the information accorded and if it is found that the user has the access right, the file access is performed.

[0008]

Moreover, when a request for access is made, the access right confirming means 13 reads the domain name from the requested file, and if the domain name registered in the apparatus itself is in accord with the domain name read from the requested file and if it is found that the user has the access right, the file access is performed.

[0009]

Furthermore, when a request for access is made, the access right confirming means 13 reads the domain name and the security information from the requested file. If the domain name registered in the apparatus itself is in accord with the domain name read from the requested file, the access right confirming means 13 collates the input information and the security information read from the requested file. If the information accorded and if it is found that the user has the access right, the file access is performed.

[0010]

Still furthermore, when a request for access is made, the access right confirming means 13 reads the security information from the requested file. If the input user ID is in accord with the owner ID read from the requested file, the access right confirming means 13 collates the input group name and the group name read from the requested file. If the group name accorded, and if the group has the access right,

the file access is performed.

[0011]

Accordingly, the security information such as owner ID, group name, access right of the group, and domain name are written in the respective files, and the information is checked by the access right confirming means 13, and thus the information processor without security device can manage the security.

[0012]

[Embodiments of the Invention]

Next, a detailed description will be given of the embodiments and operations of the present invention with reference to Figs.1 through 8.

[0013]

Fig.1 shows a block diagram of the system according to the present invention. The server 1 where the files are managed is connected to a client 11 or a plurality of clients 11 through the circuit, and the server 1 here comprises the right checking means 2.

[0014]

When the client 11 is connected to the server 1 through the circuit, the right check means 2 checks the user right, for example, by user ID and the pass word.

[0015]

The file 3 stores the data managed. The user management table 4 manages the users by registering pass word and belonging group name (e.g. the general affairs division) in advance corresponding to the user ID (See Fig.2).

[0016]

The access right table 5 manages users' access rights, for example, information on the users, groups and others in each directory or in each file are stored in the access right table 5.

[0017]

The client 11 connects to the server 1 through the circuit, and each kind of the operation is performed. Here, the client 11 comprises the registering means 12 and the access right confirming means 13.

[0018]

The registering means 12 registers data, domain name, and security information in the file, and registers the domain name in the apparatus (A detailed description will be given later with reference to Figs.4 through 7).

[0019]

The access right confirming means 13 confirms the access right based on the domain name and security information stored in the file (A detailed description will be given later with reference to Figs.6 through 8).

[0020]

File 14 stores the domain name in accordance with the client 11. File 15 stores the security information (owner ID, group name, whether the group is given access right, whether the others are given access right and more) and the domain name in data.

[0021]

Fig.2 shows an example of the user management table of the present invention. As shown in Fig.2, the user management table 4 registers the following items in advance in accordance with the user ID.

[0022]

- User ID: U01
  - Pass Word: 011
  - Group Name: X
  - Others

The user ID here is an allocated unique ID for the client 11 or the users. The group name is a group which the user belong to.

[0023]

As described above, by registering the pass word and group name in the user management table 4 in advance associating with the user ID, when the client 11 is connected to server 1 through the circuit and the client or user tries

to download the data of file 3, and when the right checking means 2 checks the right and the right is found valid, it becomes possible to download the file and the security information (owner ID, group name, whether the group is given access right, whether the others are given access right and more).

[0024]

Fig.3 is an example of the access right table according to the present invention. The access right table 5 stores in advance the security information (owner ID, group name, whether the group is given access right, whether the others are given access right and more) on each directory and the security information (owner ID, group name, whether the group is given access right, whether the others are given access right and more) on each file on file 3 where the server 1 manages the security.

[0025]

As above described, according to the file managed by the server 1, the security is managed by attaching the security information on each directory and the security information on each file, and when the file is downloaded to the client 11, the above security information is sent by being attached to the data of the file. The client 11 which receives the file keeps the security information attached to the data in the file.

[0026]

Next, according to the steps shown in the flow

chart of Fig.4, a detailed description will be given of the following steps of the system where the configuration is based on Figs.1 through 3: A file is downloaded from the server 1 to the client 11, and the security information is written in said file.

[0027]

Fig.4 is a flow chart of downloading (writing the security information) according to the present invention. According to Fig.4, the user connects the server and the user authorization is performed in S1. The client 11 connects to the sever 1 through the circuit, sending the input user ID and the pass word, then the right checking means 2 of the server 1 registers the password in accordance with user ID with reference to the user management table 4 and check whether the user has the access right or not. If the user is authorized, the procedure proceeds to S2.

[0028]

In S2, the file is received. As the access right is authorized in S1, the server 1 downloads the file 3 and the client 11 receives the file.

[0029]

In S3, the security information is received. After the file is downloaded by the server 1 and received by the client 11 in S2, with reference to the access right table 5 of the file which the server 1 downloaded, the following security information is downloaded and received by the client 11:

- User ID: A
- Group Name: X
- Whether the Group has the Access Right: Yes/No
- Whether the Other Group has the Access Right: Yes/No
- Others

Here, as for the security information, in reference with the access right table 5 shown in Fig.3, the server 1 reads both of the directory of the downloaded file and the security information of said file, and then generates more strict values (values obtained by the AND condition), and then the values are downloaded to the client 11 as security information. Accordingly, the security information is delivered from the server 1 with complete security management to the client 11 without security management.

[0030]

In S4, the security information is written in the file. The security information received in S3 is written in the file received by the client 11 in S2.

[0031]

Accordingly, the client 11 downloads the security information from the server with complete security management, and the client 11 writes said security information in the file itself so as to complete the preparation for the security management.

[0032]

Fig.5 is a flow chart of downloading (writing the

domain name) according to the present invention. Here the domain name is registered in advance. For example, the administrator who booted the client 11 inputs the domain name from the screen so as to register the domain name, "sales division" in the file 14 of client 11. According to this, the users are locked so as to access the files having only the same domain name.

[0033]

In Fig.5, the client connects to the server. Then the access right of the client is checked as well as the case described in S1 of Fig.4. If the access right is found valid, the procedure proceeds to S12. A file is received in S12. This means the client 11 receives the file from the server 1.

[0034]

The client creates a file in S13. In S14, a domain name is written in the file. This means the domain name is written in the file which is downloaded from the server 1 and then received by the client 11 in S12, or in the file created by the client 11 in S13. As for the domain name, for example as shown in Fig.9 which will be described later, "Sales Division", "General Affairs Division", and "Account Division" are written in the respective files as the domain name permitting users to access said files, and the access for the files where said domain name is written can be managed by the access right checking means 13 of the client 11 so as to enable the files to be accessed by only the clients 11 where the same domain name is registered in advance.

[0035]

Accordingly, by writing the domain name in the downloaded file or the created file, the file access can be controlled by the access right checking means 13 so as to enable the files to be accessed by only the clients (terminals) 11 where said domain name is registered.

[0036]

Fig.6 is a flow chart of access for the downloaded file according to the present invention. In S22 of Fig.6, the client connects to the server. Then the user authorization is performed. This means the client 11 connects to the server 1 through the circuit, inputs the user ID and pass word and sends them, then the access right checking means 2 of the server 1 checks the access right with reference to the user management table 4 wherein the pass word is registered in accordance with the user ID. If it is found that the access right is given to the user, the procedure proceeds to S23.

[0037]

In S23, the group name to which user ID belongs is received. This means the client 11 receives the name of group to which the user ID belongs with reference to the user management table 4 as described in Fig.2.

[0038]

In S24, the client disconnects from the server. According to S21 through S24 above, the client (terminal) 11

receives the group name of said user ID from the server.

[0039]

In S25, the client accesses to the desired file. This means user having some user ID tries to access a file 15 stored in the client 11. In S26, whether the domain names accord or not is determined. This means it is determined whether the domain name written in the file 15 user tried to access and the domain name registered in advance in said client (terminal) 11 by the administrator accord or not. In case of YES, the procedure proceeds to S27. In case of NO, the domain names do not accord, and access for said file can not be permitted, thus the access is denied in S33, the error operation is performed in S34, and the procedure ends.

[0040]

In S27, whether the user ID and the owner in the file accords or not is determined. This means it is determined whether the access right is valid or not by comparing the user ID of the user who tried to access the file and the owner ID written in the file which user tried to access. In case of YES, the access right is found valid, thus access is permitted in S31, and then the file is accessed by user in S32. On the other hand, in case of NO in S27, the user is found different from the owner, the procedure proceeds to S28.

[0041]

In S28, whether the group name and the group name in the file accord or not is determined. This means it is

determined whether the group name received in S23 wherein the user ID belongs to the group, and the group name written in the accessed file in S25 accord or not. In case of YES in S28, the client further reads whether the access right of the group written in the file is valid or not in S29. If the right is valid, the access is permitted in S31, thus the file is accessed in S32. If the right is invalid, the access is denied in S33, the error operation is performed in S34, and then the procedure ends. On the other hand, in case of NO in S28, the client moreover reads whether the access right of the other group written in the file is valid or not in S30. If the right is valid, the access is permitted in S31, thus the file is accessed in S32. If the right is invalid, the access is denied in S33, the error operation is performed in S34, and then the procedure ends.

[0042]

Accordingly, the clients (terminals) 11 without security device can manage the security in accordance with the security information the server 1 has according to the present invention by permitting the file access when the access right is found valid (in any of the following cases: YES in S27, or YES in S28 and valid in S29, or NO in S28 and valid in S30) in accordance with the domain name, owner name, group name, the access right of the group and the access right of the other group.

[0043]

Fig.7 is a flow chart of registering the domain name according to the present invention. This is a detailed procedure where the domain name is registered in advance shown

in Fig.5. In S41 shown in Fig.7, a management system is installed. According to the present step, when installing the management system (the management system such as the registering means 12 and the access right confirming means 13) on the client 11, any of the following ways of checking is registered: either the domain name or whether the security of the access right is ensured or not is checked, or both of the domain name and whether the security of the access right is ensured are checked. Accordingly, when the management system is installed, any of the following respective ways of checking the access right is set on the client: checking by the only domain name, checking by the only security information, or checking by the both domain name and security information.

[0044]

In S42, the domain name is input. In S43, the domain name is registered (the file 14 in Fig.1 is created). In the present steps: S42 and S43, the administrator installs the management system on the client (terminal) 11 so as to set the way of checking the access right (the domain name only, or the security information only, or the both of the domain name and the security information).

[0045]

Accordingly, when installing the management system on the client, the administrator can set any of the following respective ways of checking the access right: checking by the only domain name, checking by the only security information, or checking by the both domain name and security information.

[0046]

Fig.8 is a file access flow chart according to the present invention. This is a procedure of checking the access right according to the domain name. In S51 shown in Fig.8, the user tries to access the file.

[0047]

In S52, whether the domain name and the domain name in the file accord or not is determined. This means it is determined whether the domain name registered in the client 11 used by the user and the domain name written in the file which user tried to access in S51. In case of YES in S52, the domain names are found accorded and the access right is found valid, thus access is permitted in S53, and the file is accessed in S54. On the other hand, in case of NO in S52, it is found that the domain name does not accord and the user has no access right, thus the access is denied in S55, the error operation is performed in S56 and the procedure ends.

[0048]

Fig.9 is an explanatory drawing of the domain according to the present invention. Here the domain is registered in the clients (terminal) 11 used by a particular division so as to enable the clients to access the only files where said domain is registered, therefore, the clients and the files are locked by the domain name. As shown in Fig.9;

- "Domain 1" is assigned to the 3 clients (terminals) 11 of the sales division, and the same domain name "Domain 1"

is registered in said respective clients 11 according to the flow chart shown in Fig.7.

[0049]

- "Domain 2" is assigned to the 3 clients (terminals) 11 of the general affairs division, and the same domain name "Domain 2" is registered in said respective clients 11 according to the flow chart shown in Fig.7.

[0050]

- "Domain 3" is assigned to the 3 clients (terminals) 11 of the account division, and the same domain name "Domain 3" is registered in said respective clients 11 according to the flow chart shown in Fig.7.

[0051]

As above described, the domain names, "Domain 1", "Domain 2", and "Domain 3" are registered respectively in the clients (terminals) 11 used by the sales division, general affairs division, and account division according to the flow chart shown in Fig.7, thus the respective clients (terminals) 11 can access the only files out of the files in media, where each domain name accords. The other clients can not access the files when the domain name does not accord, thus it becomes possible to ensure the security.

[0052]

[Advantages of the Invention]

As above described, according to the present

invention, even the information processor without the security device can manage the security of each file since the information processor without security device adopts the following configuration wherein: the domain name and the security information such as the owner ID, group name, and access right of the group in every file, and the access right confirming means 13 checks the access right based on the above written information. Accordingly, the clients (terminals) without the security device can easily manage the file stored in media by writing the security information and the domain name in the file.

[Brief Description of the Drawings]

Fig.1 is a block diagram of the system according to the present invention.

Fig.2 is an example of the user management table according to the present invention.

Fig.3 is an example of the access right table according to the present invention.

Fig.4 is a flow chart of downloading (writing the security information) according to the present invention.

Fig.5 is a flow chart of downloading (writing the domain name) according to the present invention.

Fig.6 is a flow chart of access for the downloaded file according to the present invention.

Fig.7 is a flow chart of registering the domain name according to the present invention.

Fig.8 is a file access flow chart according to the present invention.

Fig.9 is an explanatory drawing of the domain according to the present invention.

[Description of the Reference Numbers]

1: Server

2: Right Checking Means

3: File

4: User Management Table

5: Access Right Table

11: Client (Terminal)

12: Registering Means

13: Access Right Confirming Means

14: File (Domain Name)

15: File (Data + Security Information + Domain Name)

アクセス権の有無をチェックする構成を採用しているため、ファイル毎にセキュリティを管理することができる。これらにより、セキュリティ機構を持たないクライアント（端末）であっても、ファイルにセキュリティ情報およびドメイン名を書き込んでおき、媒体などに格納されたファイルのセキュリティを簡易に管理することが可能となる。

【図面の簡単な説明】

【図１】本発明のシステムブロック図である。

【図２】本発明のユーザ管理テーブル例である。

【図３】本発明のアクセス権テーブル例である。

【図４】本発明のダウンロードフローチャート（セキュリティ情報の書き込み）である。

【図５】本発明のダウンロードフローチャート（ドメイン名の書き込み）である。

【図６】本発明のダウンロードしたファイルに対するアクセスフローチャートである。

【図７】本発明のドメイン名登録フローチャートである。

【図８】本発明のファイルアクセスフローチャートである。

【図９】本発明のドメインの説明図である。

【符号の説明】

１：サーバ

２：資格チェック手段

３：ファイル

４：ユーザ管理テーブル

５：アクセス権テーブル

１１：クライアント（端末）

１２：登録手段

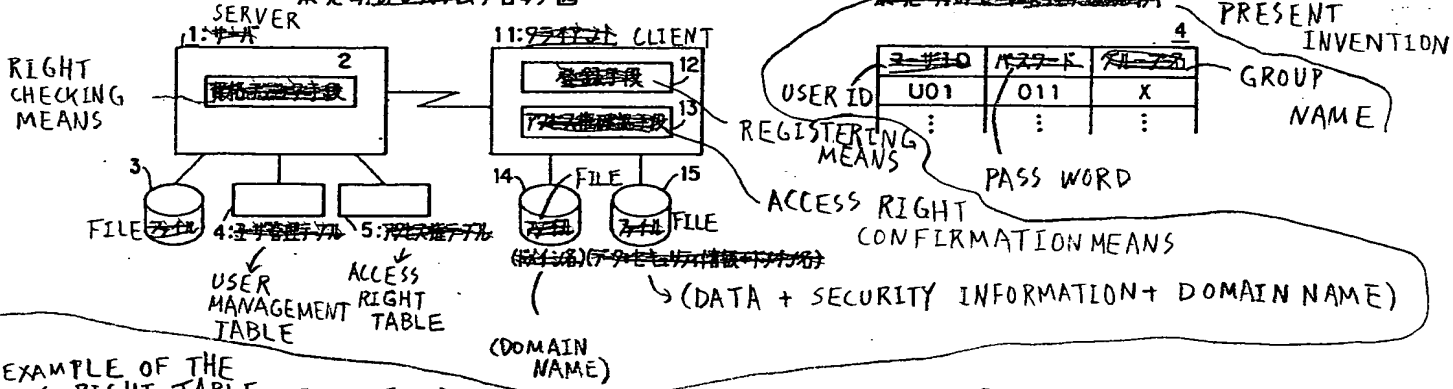
１３：アクセス権確認手段

１４：ファイル（ドメイン名）

１５：ファイル（データ＋セキュリティ情報＋ドメイン名）

【図1】 Fig.1

A BLOCK DIAGRAM OF THE SYSTEM ACCORDING TO THE PRESENT INVENTION



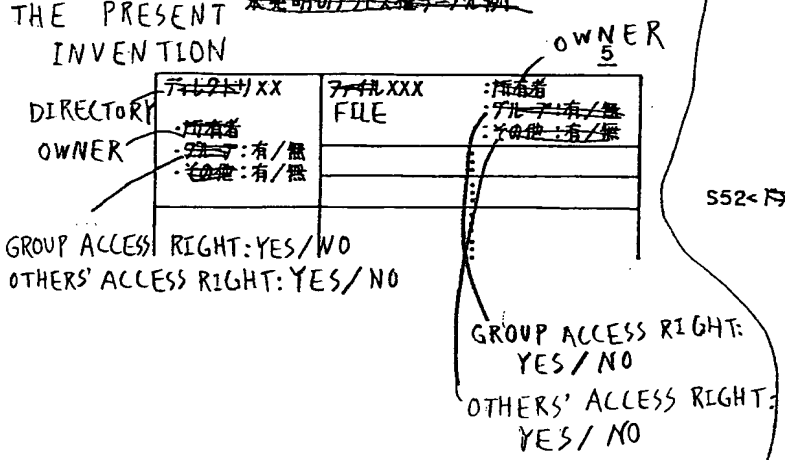
【図2】 Fig.2

AN EXAMPLE OF THE USER MANAGEMENT TABLE OF THE PRESENT INVENTION

USER ID	PASS WORD	GROUP NAME
U01	011	X
⋮	⋮	⋮

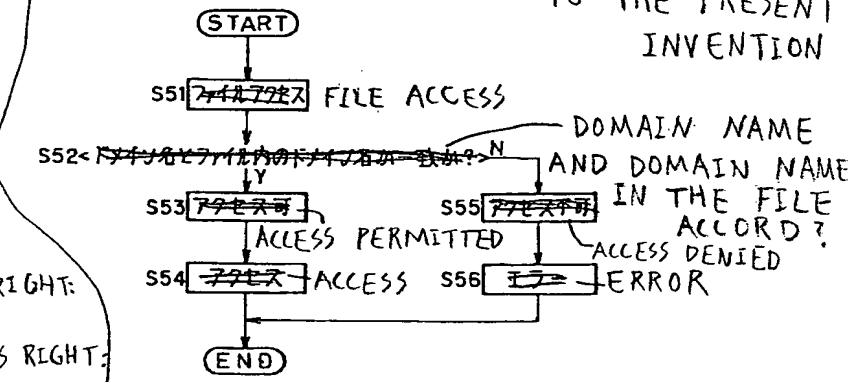
【図3】 Fig.3

AN EXAMPLE OF THE ACCESS RIGHT TABLE ACCORDING TO THE PRESENT INVENTION



【図8】 Fig.8

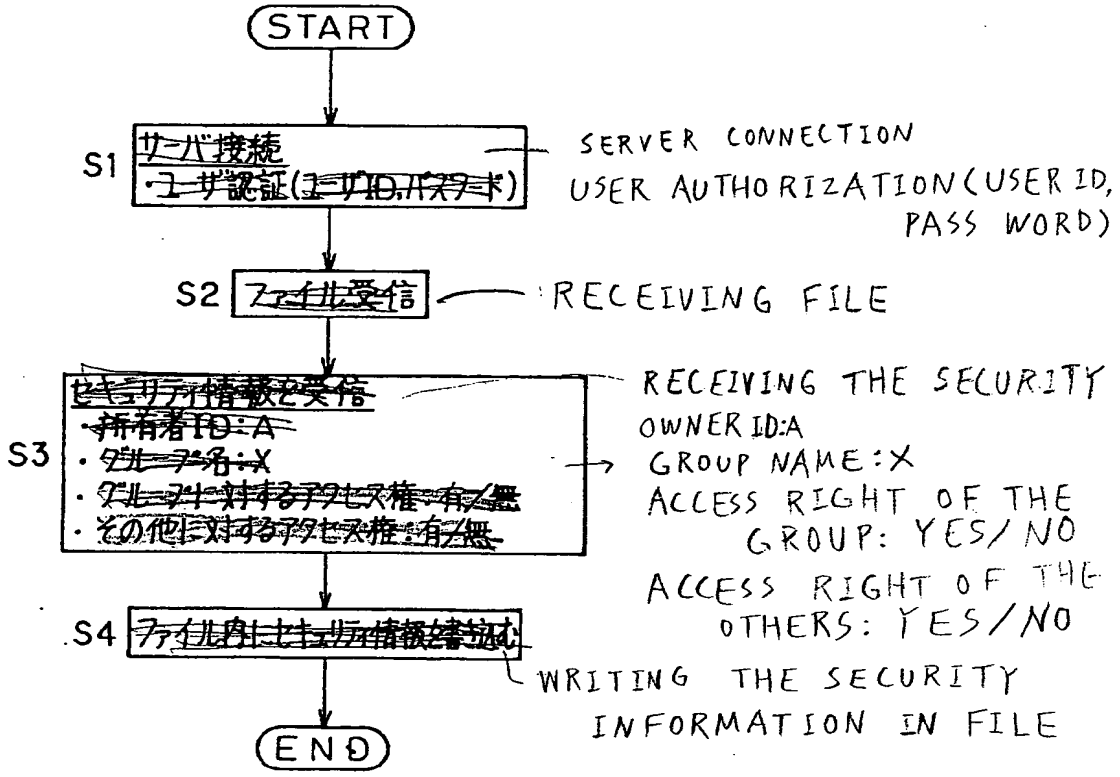
FILE ACCESS FLOW CHART ACCORDING TO THE PRESENT INVENTION



A FLOW CHART OF DOWNLOADING (WRITING THE SECURITY INFORMATION) ACCORDING TO THE PRESENT INVENTION

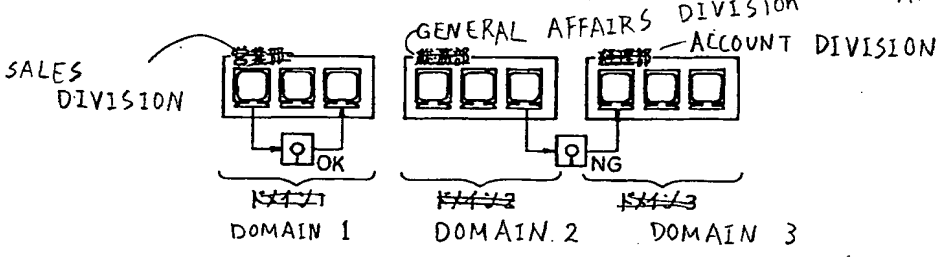
【図4】 Fig. 4

~~本発明のダウンロードフローチャート(セキュリティ情報の書き込み)~~



【図9】 Fig. 9

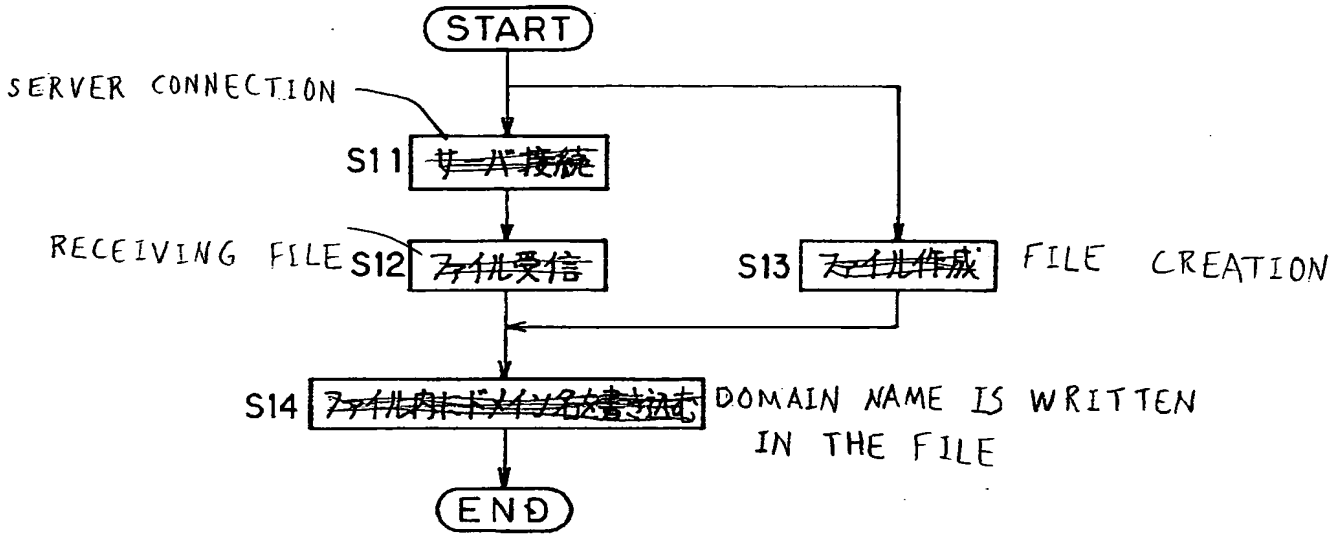
~~本発明のドメインの説明図~~ AN EXPLANATION DRAWING OF THE DOMAIN ACCORDING TO THE PRESENT INVENTION



A FLOW CHART OF DOWNLOADING (WRITING THE DOMAIN NAME) ACCORDING TO THE PRESENT INVENTION

【図5】 Fig.5

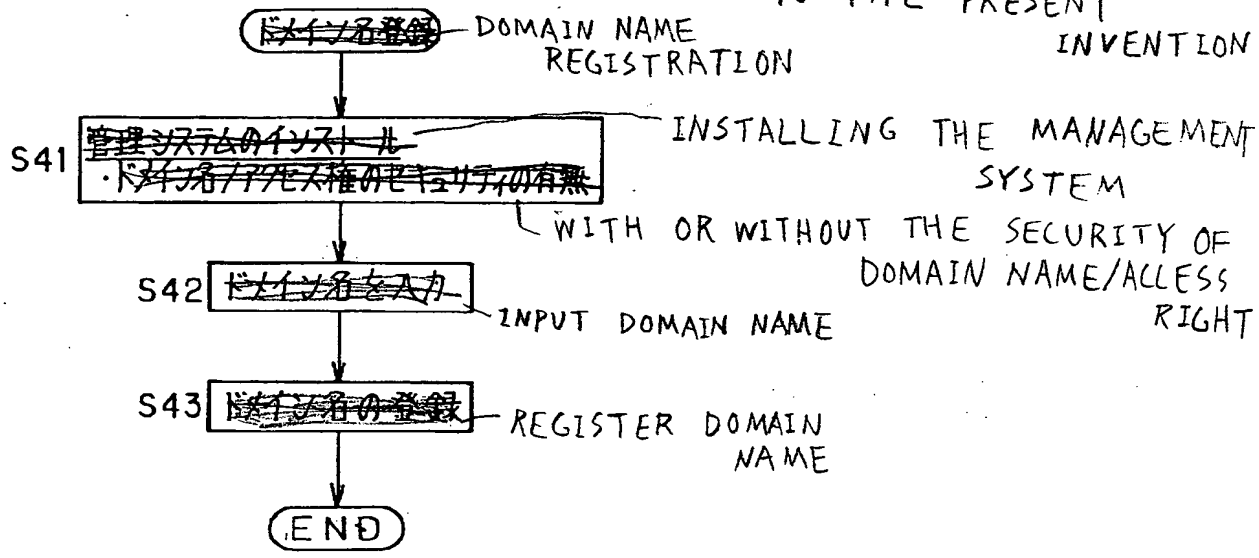
~~本発明のダウンロードフローチャート(ドメイン名の書き込み)~~



【図7】 Fig.7

~~本発明のドメイン名登録フローチャート~~

A FLOW CHART OF REGISTERING THE DOMAIN NAME ACCORDING TO THE PRESENT INVENTION



A FLOW CHART OF ACCESS FOR THE DOWNLOADED FILE ACCORDING TO THE PRESENT INVENTION

【図6】 Fig. 6

~~本発明のダウンロードしたファイルに対するアクセスフローチャート~~